

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division**

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.

Defendant.

)
)
)
)
)
)
)
)
)
)

Case No. 2:18cv00094-HCM-LRL

**MEMORANDUM IN SUPPORT OF DEFENDANT CISCO SYSTEMS, INC.'S
MOTION FOR JUDGMENT ON PARTIAL FINDINGS
PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 52(c)
AT THE CLOSE OF PLAINTIFF'S CASE**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. LEGAL STANDARDS	3
III. CENTRIPETAL HAS NOT PROVEN DIRECT INFRINGEMENT UNDER 35 U.S.C. § 271(a)	4
A. Legal Standards For Direct Infringement	4
B. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,917,856	5
1. No Literal Infringement	5
2. No Infringement Under the Doctrine of Equivalents.....	7
C. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,560,176	7
1. No Literal Infringement	8
2. No Infringement Under the Doctrine of Equivalents.....	11
D. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,137,205	12
1. No Literal Infringement	12
2. No Infringement Under the Doctrine of Equivalents.....	15
E. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,203,806	15
1. No Literal Infringement	16
2. No Infringement Under the Doctrine of Equivalents.....	21
F. Centripetal Has Failed to Prove that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,686,193	21
1. No Literal Infringement	21
2. No Infringement Under the Doctrine of Equivalents.....	25

IV.	CENTRIPETAL HAS NOT PROVED THAT CISCO INDUCED INFRINGEMENT UNDER 35 U.S.C. § 271(b)	26
V.	CONCLUSION.....	27

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Akzo Nobel Coatings, Inc. v. Dow Chem. Co.</i> , 811 F.3d 1334 (Fed. Cir. 2016)	25
<i>Centillion Data Sys. v. Qwest Commc'ns Int'l, Inc.</i> , 631 F.3d 1279 (Fed. Cir. 2011)	4, 5
<i>Chih-Wen Chung v. Bed Bath & Beyond, Inc.</i> , No. EP-09-CV-330-FM, 2011 WL 6439352 (W.D. Tex. July 1, 2011)	19
<i>Colonial Penn Ins. v. Market Planners Ins. Agency Inc.</i> , 157 F.3d 1032 (5th Cir. 1998)	3
<i>Commil USA, LLC v. Cisco Sys., Inc.</i> , 135 S. Ct. 1920 (2015)	3, 26, 27
<i>Deepsouth Packing Co. v. Laitram Corp.</i> , 406 U.S. 518 (1972)	4
<i>DSU Med. Corp. v. JMS Co.</i> , 471 F.3d 1293 (Fed. Cir. 2006)	27
<i>Ecolab, Inc. v. FMC Corp.</i> , 569 F.3d 1335, <i>amended on reh'g in part</i> , 366 F. App'x 154 (Fed. Cir. 2009)	27
<i>Federal Ins. Co. v. HPSC, Inc.</i> , 480 F.3d 26 (1st Cir. 2007)	3
<i>First Virginia Banks, Inc. v. BP Exploration & Oil, Inc.</i> , 206 F.3d 404 (4th Cir. 2000)	3
<i>Global-Tech Appliances, Inc. v. SEB, S.A.</i> , 563 U.S. 754 (2011)	26
<i>In re Zletz</i> , 893 F.2d 319 (Fed. Cir. 1989)	19
<i>Lytle v. Household Mfg, Inc.</i> , 494 U.S. 545 (1990)	4
<i>Mylan Institutional LLC v. Aurobindo Pharma Ltd.</i> , 857 F.3d 858 (Fed. Cir. 2017)	5
<i>O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.</i> , 521 F.3d 1351 (Fed. Cir. 2008)	17
<i>Ritchie v. United States</i> , 451 F.3d 1019 (9th Cir. 2006)	4
<i>Rotec Indus., Inc. v. Mitsubishi Corp.</i> , 215 F.3d 1246 (Fed. Cir. 2000)	4, 14
<i>W.L. Gore & Assocs., Inc. v. Medtronic, Inc.</i> , 874 F. Supp. 2d 526 (E.D. Va. 2012), <i>aff'd</i> , 530 F. App'x 939 (Fed. Cir. 2013)	4

<i>Warner-Jenkinson Co. v. Hilton Davis Chem. Co.</i> , 520 U.S. 17 (1997)	4, 5
--	------

STATUTES, RULES, AND REGULATIONS

35 U.S.C. § 271(a)	1, 4, 14
35 U.S.C. § 271(b)	<i>passim</i>
35 U.S.C. § 271(c)	26
Fed. R. Civ. P. 50	4
Fed. R. Civ. P. 52(a)(5)	3
Fed. R. Civ. P. 52(c)	1, 3, 4

OTHER AUTHORITIES

9C Fed. Prac. & Proc. Civ. § 2573.1 (3d ed.)	4
--	---

I. INTRODUCTION

Defendant Cisco Systems, Inc. (“Cisco”) respectfully submits the following memorandum in support of its motion under Federal Rule of Civil Procedure 52(c) for entry of judgment on partial findings on the issues of direct infringement under 35 U.S.C. § 271(a) and induced infringement under 35 U.S.C. § 271(b) as to all asserted patents. Plaintiff Centripetal Networks, Inc. (“Centripetal”) has “been fully heard” on those issues, such that the Court may make findings and enter judgment against Centripetal on any or all of those issues now, which would significantly shorten the presentation of the defense case. Fed. R. Civ. P. 52(c).

Unlike in a jury trial, the Court does not take all inferences in Centripetal’s favor when deciding this motion, but rather may judge the credibility of Centripetal’s witnesses and draw reasonable inferences as the evidence warrants. As is developed in Part III below, the evidence shows that Centripetal has failed to prove that the accused combinations of Cisco’s products meet key limitations of Centripetal’s asserted patent claims, whether literally or by equivalents:

- **’856 patent:** Centripetal presented no evidence that the accused combinations “filter” or “route” “the determined packets”—i.e., the packets previously determined to comprise “encrypted data that corresponds to the one or more network-threat indicators”; the packets Centripetal pointed to indisputably proceed to their ultimate destination without interruption and thus are not “filter[ed].”
- **’176 patent:** Centripetal presented no evidence that the accused combinations “correlate” ingress and egress NetFlow records, as Centripetal’s infringement theory of the ’176 patent claims requires; Centripetal merely pointed to

documents using the buzzword “correlate,” but these documents indisputably do not discuss correlating ingress and egress NetFlow records.

- **'205 patent:** Centripetal presented no evidence that the accused combinations satisfy the various “configured to” limitations as the Court construed them; Dr. Mitzenmacher admitted that someone would still need to “set up a rule” in the accused products to perform the claimed functions, and he failed to offer any proof whatsoever regarding the limitation requiring a “network device *configured to* copy information ... and to forward the at least one packet to the destination network address.”¹
- **'806 patent:** Centripetal presented no evidence that the accused combinations “cease processing one or more packets” under the proper interpretation of that term, which means to *stop processing* one or more packets that the system has *already begun processing* under the first rule set; it is undisputed that the accused combinations do not stop processing one or more packets that the system has already begun processing under the first rule set.
- **'193 patent:** Cisco has presented no evidence that the accused combinations have “one or more packet-filtering rules configured to prevent a *particular type of data transfer*”; Centripetal’s reliance on the quarantine option fails because it is a human-operated tool rather than a “packet-filtering *rule*,” and it does not apply to any “*particular* type of data transfer.”

¹ All emphases are added unless otherwise noted.

Centripetal's assertion that Cisco *induced* a third party's direct infringement under 35 U.S.C. § 271(b) fails for an additional reason. Induced infringement requires proof that Cisco *actually knew* that the third party's actions would constitute direct infringement of Centripetal's patents. *Commil USA, LLC v. Cisco Sys., Inc.*, 135 S. Ct. 1920, 1926 (2015). Centripetal did not even attempt to prove such knowledge on Cisco's part. *See infra* Part IV.

For the foregoing reasons, the Court should enter judgment on partial findings that Centripetal has failed to prove direct infringement of all asserted patents and has likewise failed to prove induced infringement of all asserted patents.

II. LEGAL STANDARDS

"If a party has been fully heard on an issue during a nonjury trial and the court finds against the party on that issue, the court may enter judgment against the party on a claim or defense that, under the controlling law, can be maintained or defeated only with a favorable finding on that issue." Fed. R. Civ. P. 52(c). Rule 52(c) "authorizes the court to enter judgment at any time that it can appropriately make a dispositive finding of fact on the evidence." *First Virginia Banks, Inc. v. BP Exploration & Oil, Inc.*, 206 F.3d 404, 407 (4th Cir. 2000) (internal quotation marks omitted). The Court may issue judgment under Rule 52(c) "with respect to issues or defenses that *may not be wholly dispositive of a claim or defense*." Fed. R. Civ. P. 52(c) Advisory Committee's Note to 1993 Amendment (emphasis added).²

² Cisco reserves the right to challenge any factual findings made as to other issues not addressed in this motion. *See* Fed. R. Civ. P. 52(a)(5) ("A party may later question the sufficiency of the evidence supporting the findings, whether or not the party requested findings, objected to them, moved to amend them, or moved for partial findings."); *Federal Ins. Co. v. HPSC, Inc.*, 480 F.3d 26, 32 (1st Cir. 2007); *Colonial Penn Ins. v. Market Planners Ins. Agency Inc.*, 157 F.3d 1032, 1036-37 & n.3 (5th Cir. 1998).

In deciding Cisco's Rule 52(c) motion, the Court should weigh the evidence and may make inferences in Cisco's favor. *W.L. Gore & Assocs., Inc. v. Medtronic, Inc.*, 874 F. Supp. 2d 526, 540 (E.D. Va. 2012) ("To grant JMOL under Rule 52(c), a district judge must weigh the evidence and resolve credibility."), *aff'd*, 530 F. App'x 939 (Fed. Cir. 2013). In contrast to judgment as a matter of law in a jury trial under Fed. R. Civ. P. 50, "[i]n deciding whether to enter judgment on partial findings under Rule 52(c), the district court is not required to draw any inferences in favor of the non-moving party; rather, the district court may make findings in accordance with its own view of the evidence." *Ritchie v. United States*, 451 F.3d 1019, 1023 & n.7 (9th Cir. 2006) (citing *Lytle v. Household Mfg, Inc.*, 494 U.S. 545, 554 (1990) (discussing Rule 52(c)'s predecessor)); *see also* 9C Fed. Prac. & Proc. Civ. § 2573.1 (3d ed.).

III. CENTRIPETAL HAS NOT PROVEN DIRECT INFRINGEMENT UNDER 35 U.S.C. § 271(a)

A. Legal Standards For Direct Infringement

To prove direct infringement, Centripetal was required to prove by a preponderance of the evidence that Cisco made, used, sold, offered for sale within, or imported into the United States a product that meets *all* the requirements of the asserted claims while the asserted patents were in force. 35 U.S.C. § 271(a); *Warner-Jenkinson Co. v. Hilton Davis Chem. Co.*, 520 U.S. 17, 40 (1997). "[O]ne may not be held liable under § 271(a) for 'making' or 'selling' less than a complete invention." *Rotec Indus., Inc. v. Mitsubishi Corp.*, 215 F.3d 1246, 1252 & n.2 (Fed. Cir. 2000) (citing *Deepsouth Packing Co. v. Laitram Corp.*, 406 U.S. 518, 527-529, 531 (1972)); *Centillion Data Sys. v. Qwest Commc'ns Int'l, Inc.*, 631 F.3d 1279, 1288 (Fed. Cir. 2011) (finding that to "make" a system under § 271(a), a defendant must combine all of the claim elements). To "use" a system, the alleged direct infringer must "use" each and every element of

the system, and must also put the invention into service—it must be the entity that controls the system as a whole and obtains a benefit from it. *Centillion*, 631 F.3d at 1284.

If a patentee fails to demonstrate that a claim element is literally met, it may attempt to prove that that element is met under the doctrine of equivalents. *Warner-Jenkinson*, 520 U.S. at 29-30. A claim element may be met by equivalents if the accused product performs substantially the same function in substantially the same way to obtain the same result as the claim element. *Mylan Institutional LLC v. Aurobindo Pharma Ltd.*, 857 F.3d 858, 866-67 (Fed. Cir. 2017). An accused product may also meet a claim element by equivalents if it is insubstantially different from what is patented. *Id.* However, the doctrine of equivalents may not be applied so broadly as to effectively eliminate or vitiate a claim element. *Warner-Jenkinson*, 520 U.S. at 29-30.

B. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,917,856

For U.S. Patent No. 9,917,856 (the “’856 patent”), Centripetal contends that Cisco’s accused switches and routers in combination with Stealthwatch and the Identity Services Engine (“ISE”) meet the elements of claims 24 and 25. Trial Tr. (Vol. 6B) (Cole) at 886:6-11.

Centripetal has failed to present evidence sufficient to show that Cisco infringes these claims literally, and Centripetal admitted that it offered no evidence of infringement of the ’856 patent under the doctrine of equivalents. Cisco is thus entitled to judgment of non-infringement.

1. No Literal Infringement

The early limitations of asserted claims 24 and 25 require that the accused combination “receive data indicating a plurality of network-threat indicators,” “identify packets comprising unencrypted data,” and “identify packets comprising encrypted data.” Then, building on these limitations, the accused combination must

determine, based on a portion of the unencrypted data
corresponding to one or more network-threat indicators of the

plurality of network-threat indicators, *packets* comprising encrypted data that corresponds to the one or more network-threat indicators

JTX-5 at claims 24, 25. Later, the accused combination must “*filter ... the determined packets* comprising the encrypted data that corresponds to the one or more network-threat indicators.” In other words, the accused combination must filter “*the*” very same packets that were previously “determine[d]” to contain “encrypted data that corresponds to the one or more network-threat indicators.” Then the accused combination must “*route ... filtered packets* to a proxy system.” *Id.*

The accused combination indisputably does not “filter” or “route” to a proxy system any of the packets alleged to be part of the “determine” step. Centripetal’s expert Dr. Cole testified that, in his view, the “determine” step is performed in Stealthwatch based on NetFlow records sent from the router or switch. Trial Tr. (Vol. 7B) (Cole) at 1054:10-20, 1059:13-15. But Dr. Cole admitted that *as the NetFlow record is sent to Stealthwatch, the packet continues on to its ultimate destination:*

Q. But the packets would, the packets would go from User 1 or User 2, through the router, and on to their intended destination, right?

A. *Yes. The packets as part of that connection would get routed to its destination.*

Q. Meanwhile, the NetFlow record goes up to Stealthwatch, right?

A. *The NetFlow records that are generated goes up to StealthWatch for analytics, correct.*

Q. And the NetFlow record does not go to the users, right?

A. The NetFlow – *the packets go to the user*, but the NetFlow doesn’t go to the user packets.

Trial Tr. (Vol. 8A) (Cole) at 1078:7-18; *see also id.* at 1076:1-5 (admitting that NetFlow is “routed in a different manner ... [t]han the packets”); *id.* at 1082:16-20 (admitting that “NetFlow records were sent to the StealthWatch Cloud and the packets proceeded along their way to the users as part of the communication session”); Trial Tr. (Vol. 7B) (Cole) at 1064:21-1066:6 (admitting that as the NetFlow record is sent to Stealthwatch, “the original packets that came in to the router or switch, they keep on going” to their ultimate destination). In other words, by the time Stealthwatch makes any determination about the content of a particular packet, that packet has already been transmitted from the router or switch to its ultimate destination. Certainly, Centripetal has provided no evidence that Stealthwatch (or any other component of the accused combination) ever “filter[s] ... the determined packets” or “route[s] ... filtered packets to a proxy system,” as the claims require. Instead, all of the alleged “determined packets” proceed to their ultimate destination long before Stealthwatch makes any determination about them.

2. No Infringement Under the Doctrine of Equivalents

Although Centripetal asserted infringement under the doctrine of equivalents for the ’856 patent in its Amended Complaint and in the Pre-Trial Order (Dkt. 29 ¶¶ 63, 357, 388, 391; Dkt. 408 at 18 ¶ 20), it did not even attempt to introduce any evidence of infringement by equivalents for this patent at trial. Centripetal’s counsel admitted as much when asked by the Court. Trial Tr. (Vol. 8A) at 1087:13-1088:7. Thus, Cisco is entitled to judgment that the ’856 patent is not infringed by equivalents.

C. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,560,176

For U.S. Patent 9,560,176 (the “’176 patent”), Centripetal contends that the combination of Cisco’s accused switch or router along with Stealthwatch with Cognitive Threat Analytics (“CTA”) meets the elements of claims 11 and 21. Trial Tr. (Vol. 7A) (Cole) at 975:19-21.

Centripetal has failed to present evidence sufficient to show that Cisco infringes these claims literally, and Centripetal admitted that it offered no evidence of infringement of the '176 patent under the doctrine of equivalents. Cisco is thus entitled to judgment of non-infringement of the '176 patent.

1. No Literal Infringement

Asserted claims 11 and 21 require a system or a non-transitory computer-readable medium that, inter alia, does each of the following things:

identify a plurality of packets received by a network device from a host located in a first network;

generate a plurality of log entries corresponding to the plurality of packets received by the network device;

identify a plurality of packets transmitted by the network device to a host located in a second network;

generate a plurality of log entries corresponding to the plurality of packets transmitted by the network device;

correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device.

JTX-3 at claims 11, 21. Importantly, the “correlate” limitation requires a specific kind of correlation, namely correlation of “the plurality of packets transmitted by the network device” with “the plurality of packets received by the network device,” “*based on* [1] the plurality of log entries corresponding to the plurality of packets received by the network device and [2] the plurality of log entries corresponding to the plurality of packets transmitted by the network device.” *Id.* (bracketed numerals added for clarity).

Centripetal failed to present any evidence that the accused combination performs these specific requirements of the “correlate” limitation. According to Dr. Cole, the two sets of log entries that must be correlated (i.e., “the plurality of log entries corresponding to the plurality of packets *received* by the network device and the plurality of log entries corresponding to the plurality of packets *transmitted* by the network device”) are two sets of *NetFlow records* (ingress and egress) sent from the accused router or switch to Stealthwatch. *See* Trial Tr. (Vol. 8A) (Cole) at 1102:25-1103:7 (“Q. And so [claim element] B2 would be the ingress NetFlow record; is that fair? A. That looks to be correct, yes. A. And [claim element] B4 would be the egress NetFlow record; is that fair? A. That would also be correct. Q. Okay. And then those NetFlow records are going to be sent up to StealthWatch; is that fair? A. That is my understanding.”); *id.* at 1106:5-8 (“Q. And the claim specifically requires that it be the two NetFlow records that you identified be correlated, fair? A. The claim says that you’re correlating the logs from B2 and the logs from B4.”); *id.* at 1108:4-5 (claims require that “those two NetFlow records are being correlated”). According to Dr. Cole, when a packet is received by an accused router or switch, a corresponding “ingress” (“input”) NetFlow record is sent to Stealthwatch; and when that packet is transmitted from the accused router or switch, a corresponding “egress” (“exit”) Netflow record is sent to Stealthwatch. Trial Tr. (Vol. 7A) (Cole) at 980:4-16, 983:21-25, 984:19-24, 986:12-987:1, 988:17-989:1, 989:25-990:8; Trial Tr. (Vol. 8A) (Cole) at 1102:5-15, 1102:25-1103:7.

Crucially, however, Centripetal offered *no evidence whatsoever* that the accused combination *ever* compares ingress and egress NetFlow records to correlate their ingress and egress log entries, as Dr. Cole’s theory of the “correlation” limitation required. Dr. Cole relied

on three exhibits for this limitation, but they merely use variants of the word “correlate” to refer to very different actions; none demonstrates the specific type of correlation recited in the claims.

First, Dr. Cole relied on PTX-1065, which is an internal Cisco presentation titled “Cisco Stealthwatch with Cognitive Threat Analytics.” Trial Tr. (Vol. 7A) (Cole) at 994:2-9; PTX-1065. Focusing on page 5 of the document (Bates 00037337.0005), Dr. Cole highlighted language stating “the cloud-based analytics engine that *correlates threat behavior* seen in the enterprise with those seen globally.” Trial Tr. (Vol. 7A) (Cole) at 995:13-18; PTX-1065 at 5. However, this language—*which does not even mention NetFlow*—is discussing a correlation of threats “seen in the enterprise” (i.e., within the Cisco-protected system) with threats “seen globally” (i.e., outside the Cisco-protected system). PTX-1065 at 5. It is not talking about correlating a log entry for a packet received by a router/switch with a log entry for a packet transmitted by that router/switch, much less performing such a correlation “based on” an ingress NetFlow record and an egress NetFlow record. This document provides no support for Dr. Cole’s opinion on the “correlate” limitation.

Second, Dr. Cole relied on PTX-591, which shows release notes for Stealthwatch version 6.10.3. Trial Tr. (Vol. 7A) (Cole) at 996:5-10; PTX-591. Focusing on page 4 of this document (Bates 065522), Dr. Cole highlighted language stating “CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through *correlation of both telemetry types*.” PTX-591 at 4; Trial Tr. (Vol. 7A) (Cole) at 996:17-997:5. Again, this document is discussing an entirely different kind of “correlation” from that recited in the claims. The language of PTX-591 on its face is talking about correlation of *two different* “telemetry types”—WebFlow and NetFlow—not comparing ingress *NetFlow* records to egress *Netflow* records to correlate

received and transmitted packets, as Dr. Cole’s infringement theory requires in the context of the “correlate” claim limitation. For this reason, Dr. Cole was unable to identify anywhere in the document that actually discussed correlating ingress NetFlow records with egress NetFlow records. Trial Tr. (Vol. 8A) (Cole) at 1109:7-19.

Finally, Dr. Cole relied on identical language from PTX-1009, which shows release notes for Cognitive Intelligence (formerly CTA). Trial Tr. (Vol. 7A) (Cole) at 997:13-21; PTX-1009. Dr. Cole focused on page 9 of this document (Bates 00004105.0009), which states “CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through *correlation of both telemetry types*.” PTX-1009 at 9; Trial Tr. (Vol. 7A) (Cole) at 997:23-998:17. This is the exact same language Dr. Cole relied on for PTX-591 (Trial Tr. (Vol. 8A) (Cole) at 1110:3-6)—and it fails to show the claimed correlation for the same reason.

Dr. Cole cannot simply cherry-pick the word “correlation” from various Cisco documents; the claims specifically require correlation of *packets* received and transmitted from an accused device based on the *log entries* generated upon a packet’s ingress and egress. None of his documents remotely suggests that Cisco’s devices perform that specific form of correlation to which the claims are limited. And he tellingly could not remember any source code that he had pointed to that suggested otherwise (Trial Tr. (Vol. 8A) (Cole) at 1110:7-16)—a point Centripetal’s counsel did not attempt to address on redirect examination.

In sum, because Dr. Cole’s opinion that the accused combination “correlates” received and transmitted packets based on their ingress and egress log entries is not supported by any evidence, Cisco is entitled to judgment of no literal infringement of the ’176 patent.

2. No Infringement Under the Doctrine of Equivalents

Although Centripetal asserted infringement under the doctrine of equivalents for the '176 patent in its Amended Complaint and in the Pre-Trial Order (Dkt. 29 ¶¶ 63, 104, 127, 130; Dkt. 408 at 18 ¶ 21), it did not even attempt to introduce any evidence of infringement by equivalents for this patent at trial. As with the '856 patent, Centripetal's counsel admitted its failure of proof under the doctrine of equivalents when asked by the Court. Trial Tr. (Vol. 8A) at 1087:13-1088:7. Thus, Cisco is entitled to judgment of no infringement by equivalents for the '176 patent.

D. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,137,205

Centripetal contends that the accused product combinations (accused switches with Digital Network Architecture ("DNA"), accused routers with DNA, and accused firewalls with Firepower Management Center ("FMC")) meet the limitations of claims 63 and 77 of U.S. Patent No. 9,137,205 (the "'205 patent"). Centripetal's Findings of Fact ¶¶ 246-248 (Dkt. 419); Trial Tr. (Vol. 6A) (Mitzenmacher) at 725:14-726:10. Centripetal has failed to provide sufficient evidence to show infringement of these claims, either literally or under the doctrine of equivalents, because the accused combinations are not "configured to" perform the functions recited in the asserted claims, as the Court construed that limitation in its Claim Construction Order. Cisco is thus entitled to judgment of non-infringement.

1. No Literal Infringement

Both asserted claims 63 and 77 require a system or a non-transitory computer-readable medium that, inter alia, does the following:

receive, from the security policy management server, a dynamic security policy comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol (SIP) Uniform Resource Identifier (URI);
receive packets associated with a network protected by the packet security gateway;

perform, on the packets, on a packet by packet basis, at least one packet transformation function of multiple packet transformation functions specified by the dynamic security policy;

encapsulate at least one packet of the packets that falls within the set of network addresses and matches the SIP URI with a header containing a network address that is different from a destination network address specified by the at least one packet and that corresponds to a ***network device configured to copy information*** contained in the at least one packet and to forward the at least one packet to the destination network address; and

route, based on the header, the at least one packet to the network address that is different from the destination network address.

JTX-1 at claims 63 and 77. Claim 63 of the '205 patent specifically recites a “packet security gateway” that is “***configured to***” perform the recited actions listed above (*e.g.*, to “receive...a dynamic security policy...”). *Id.* Both asserted claims 63 and 77 also require a “network device ***configured to*** copy information contained in the at least one packet and to forward the at least one packet to the destination network address.” *Id.*

The Court construed the phrase “configured to” in the '205 patent claims to require that the accused devices be configured to ***actually perform*** the recited functions, not that the devices merely be capable of performing those functions if a human later configured them to do so. *See* Dkt. 202 at 14 (“configured to” “requires that the device be actually configured to do the function” (emphasis in original)); *id.* at 22 (“configured to” “requires that the action actually do the function ***automatically***”); Dkt. 191, *Markman* Tr. at 39:13-22 (“COURT: I think the language speaks for itself, so I think it means that ***it does it, not just is capable of doing it...*** I think the way it’s used in the claim language, ***it means it shall do that, not that it’s capable.***”).

Centripetal presented no evidence that the accused product combinations have ever been “actually configured to do the function[s]” required by the claims. Dr. Mitzenmacher admitted that he did not recall presenting any such evidence, and notably, Centripetal’s counsel did not elicit any redirect testimony from Dr. Mitzenmacher bearing on the “configured to” limitation as

the Court construed it. *See* Trial Tr. (Vol. 6B) (Mitzenmacher) at 863:5-17 (“Q. You haven’t shown us any examples of where someone actually set up a rule to do this, right? A. Set up an example? I don’t recall specifically showing that.”); *id.* at 861:22-862:10 (“***I can’t recall***” identifying “a rule that has, as the condition, the presence of a [SIP URI], as the condition, and the result being if it’s got that SIP URI address, then it will encapsulate the packet”); *id.* at 870:22-871:11. Instead, Dr. Mitzenmacher testified that, in his view, he only needed to demonstrate that the accused product combinations contained “code” or “functionality” that would allow someone to “set up a rule” that would perform the actions recited in the claim. *See id.* at 863:8-9 (“You know, ***someone may have to set up a rule to do it***, but the system has the code to do all this”); *see also generally id.* at 862:16-863:17, 870:22-871:11. That is not enough under the Court’s claim construction, which limits the claimed invention to a device “actually configured” to perform the recited functions. Dkt. 202 at 14 (emphasis in original). The claims are not infringed by a device that merely ***could be*** so configured if someone “set[s] up a rule to do it.” *See, e.g., Rotec*, 215 F.3d at 1252 n.2 (“[O]ne may not be held liable under § 271(a) for ‘making’ or ‘selling’ less than a complete invention.”); Trial Tr. (Vol. 6B) (Mitzenmacher) at 863:8-9.

Moreover, Dr. Mitzenmacher essentially ignored the requirement of a “network device ***configured to*** copy information ... and to forward the at least one packet to the destination network address,” which is present in the second part of the “encapsulate” limitation of asserted claims 63 and 77. JTX-1 at claims 63 and 77. While Dr. Mitzenmacher briefly testified about what this language requires (Trial Tr. (Vol. 6A) (Mitzenmacher) at 758:11-21), he offered ***no testimony whatsoever*** purporting to show that Cisco’s accused combination satisfied that requirement. *See generally* Trial Tr. (Vol. 6A) (Mitzenmacher) at 756:8-767:6. Indeed, Dr.

Mitzenmacher did not even *identify* the claimed “network device,” much less explain how any such device is “configured to” perform the claimed “copy” and “forward” functions. *Id.* Having not discussed how this requirement is met, Dr. Mitzenmacher also necessarily ignored, yet again, this Court’s claim construction of “configured to” by failing to present any evidence that any alleged network device is “actually configured” to perform the required operations to “copy” and “forward.” Dkt. 202 at 14 (emphasis in original). Centripetal thus failed to demonstrate that the accused product combinations are configured to perform the functions that the asserted claims require.

In sum, because Dr. Mitzenmacher failed to offer any evidence that the accused combinations were ever configured to actually perform the required operations of the asserted claims, and because he failed to offer any evidence whatsoever for the “network device configured to copy” limitation, Cisco is entitled to judgment of no literal infringement of the ’205 patent.

2. No Infringement Under the Doctrine of Equivalents

For the ’205 patent, Centripetal only referenced the doctrine of equivalents for the “SIP URI” limitation of the asserted claims. *See generally* Trial Tr. (Vol. 6A) (Mitzenmacher) at 774:2-775:12. Thus, Centripetal’s equivalents argument cannot cure the deficiencies of proof for the “configured to” limitations relied upon in this motion.

E. Centripetal Has Not Shown that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,203,806

Centripetal contends that the accused product combinations (accused switches with DNA; accused routers with DNA; and accused firewalls with FMC) meet the limitations of claims 9 and 17 of U.S. Patent No. 9,203,806 (the “’806 patent”). Centripetal’s Findings of Fact ¶¶147-149 (Dkt. 419); PTX-1883; Trial Tr. (Vol 4) (Mitzenmacher) at 556:11-557:4. Centripetal has

failed to provide sufficient evidence to show infringement of these claims, either literally or under the doctrine of equivalents, because the accused routers, switches, and firewalls do not meet the “cease processing of one or more packets” limitation. Cisco is accordingly entitled to judgment of non-infringement.

1. No Literal Infringement

Asserted claims 9 and 17 require a system or a non-transitory computer-readable medium that, inter alia, does the following:

process, in accordance with the first rule set, a portion of the plurality of packets;

signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and

configure, each processor of the at least two processors to, responsive to being signaled to process packets in accordance with the second rule set:

cease processing of one or more packets;

cache the one or more packets;

reconfigure to process packets in accordance with the second rule set;

signal completion of reconfiguration to process packets in accordance with the second rule set; and

responsive to receiving signaling that each other processor of the at least two processors has completed reconfiguration to process packets in accordance with the second rule set, *process, in accordance with the second rule set, the one or more packets.*

JTX-2 at claims 9 and 17. The '806 patent's asserted claims require a specific sequence of actions to be performed on “one or more packets.” First, the system must receive and “*process, in accordance with the first rule set, a portion of the plurality of packets.*” The claims then require that the accused combinations “*cease processing* of one or more packets” and, later, “process, in accordance with the second rule set, the one or more packets.” Accordingly, the

system must cease processing one or more packets and then, later, process *those same packets* with the second rule set.

a. The Court Should Resolve the Parties’ Dispute Over the Proper Construction of the “Cease Processing of One Or More Packets” Limitation

Centripetal’s case-in-chief has revealed that the parties dispute the proper construction of “cease processing of one or more packets” in the asserted claims. Cisco’s interpretation of this term all along (including as set forth in its summary judgment brief, Dkt. 260 at 5-8) has been the term’s plain meaning: that “cease processing of one or more packets” means to *stop processing* one or more packets that the system has *already begun processing* under the first rule set. Dr. Mitzenmacher’s testimony demonstrated, however, that Centripetal seeks to interpret this term more broadly—namely, to cover implementations in which the system does *not* start processing a particular packet and then stop processing the same packet. Rather, Centripetal appears to read the claim to require only that the claimed system does not *begin* processing any *new* packets under the first rule set after the system is signaled to process packets in accordance with the second rule set. *See* Trial Tr. (Vol 5A) (Mitzenmacher) at 619:25-620:16 (“So what you have to do is stop processing *for anything coming in*, and anything that you would normally process, you’re going to cache.”). Put another way, under Centripetal’s reading, no *cessation* of processing the “one or more packets” is required.

Accordingly, the parties have a claim construction dispute that must be resolved as a legal matter before the Court can decide literal infringement as a factual matter. *See O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1361-63 (Fed. Cir. 2008) (noting that “[a] determination that a claim term ‘needs no construction’ or has the ‘plain and ordinary meaning’ may be inadequate when a term has more than one ‘ordinary’ meaning or when

reliance on a term's 'ordinary' meaning does not resolve the parties' dispute"; and remanding to the district court to undertake the court's "duty" to construe a disputed claim term).

Cisco's interpretation is supported by the claim's plain language. The plain meaning of "cease" is to stop or discontinue. A product cannot *cease* processing a packet that it *never started* processing. The specification further supports Cisco's understanding. As noted above, the next function required by the claims after the "cease processing" limitation is to "cache" the very same "one or more packets" that the system had just "cease[d] processing." JTX-2 at claims 9 and 17. When introducing the concept of caching a packet, the '806 patent specification states that "each of processors 300, 302, and 304 may *cease processing packets and cache the packet they are currently processing* for future processing in accordance with policy 132's rule set." JTX-2 at 7:59-63. This language clearly demonstrates that the patent contemplates ceasing processing of packets that are currently being processed, rather than simply not processing any new packets as Centripetal appears to believe.

The prosecution history further supports Cisco's interpretation. During prosecution of the '806 patent, Centripetal added the second half of the claims, including the "cease processing" limitation, to overcome prior art. Ex. A³ ('806 patent prosecution history, October 6, 2015 Amendment) at 2-4, 6 (amending claims 26 (which issued as asserted claim 9) and 34 (which issued as asserted claim 17)).⁴ Centripetal argued that the amended claims distinguished over prior art (Narayanaswamy) that held packets for processing in a queue because, unlike the

³ Citations herein to Exhibits A-L are to exhibits attached to and in support of this motion.

⁴ The October 6, 2015 Amendment was an exhibit to Cisco's summary judgment motion. Dkt. 260, Ex. 5. Because this exhibit is intrinsic evidence relevant to the "cease processing" claim construction dispute, Cisco resubmits this exhibit (as Ex. A) with this motion.

asserted claims, these queues did not “*cache packets for which processing has ceased.*” *Id.* at 13-14. The Examiner then allowed the claims in part due to Centripetal’s addition of the “cease processing” limitation. Ex. B (’806 patent prosecution history, October 16, 2015 Notice of Allowability) at Bates 001293-94 (“The following is an examiner’s statement of reasons for allowance: The prior art ... fails to explicitly teach ... cease processing of one or more packets; cache the one or more packets”). Centripetal should be held to the claim interpretation it used to have the asserted claims granted. *See, e.g., In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989) (“When the applicant states the meaning that the claim terms are intended to have, the claims are examined with that meaning.”); *Chih-Wen Chung v. Bed Bath & Beyond, Inc.*, No. EP-09-CV-330-FM, 2011 WL 6439352, at *8 (W.D. Tex. July 1, 2011) (adopting the proposed construction that tracked the patent applicant’s express language in the prosecution history).

b. Under the Proper Construction of “Cease Processing of One Or More Packets,” Centripetal Has Failed to Prove Literal Infringement

Centripetal has failed to show that the accused product combinations “cease processing of one or more packets,” as that limitation is properly construed. Centripetal offered no evidence that the accused product combinations *cease processing* any packet after having begun processing it with the first rule set, and then begin processing that same packet with a second rule set. Instead, as Dr. Mitzenmacher admitted and Cisco’s technical documents confirm, if the Cisco accused products start processing any packets with a first rule set, they continue to process those packets under the first (“old”) rule set during the rule swap. Trial Tr. (Vol. 6A) (Mitzenmacher) at 816:7-19 (confirming that when the new rule set arrives, the Cisco products keep using the old rule sets “for the time that it takes in order to prepare a packet”); *id.* at 822:13-22 (confirming that the products continue using the old rules for a short time during the “very minimal delay of the compilation” of the new rules); *id.* at 823:24-824:10; DTX-1290 (Bates

00006892.0668-0669) (including a table establishing that the accused products do not cease processing packets while “implementing rule changes”; the accused “transactional” products match old rules while new rule sets are compiling, whereas older systems matched the new rule sets while the new rules were compiling); PTX-1196 (Bates 00008406.0007-0008) (“with the proposed transactional-commit model, new rules will not take effect until compilation is done and stable. ***During compilation, packets will still match the old set of rules***”); *see also* Trial Tr. (Vol. 6B) (Mitzenmacher) at 830:18-22 (showing that the transactional-commit model is accused by Centripetal). The second rule set in the accused combinations is then only applied to packets for which processing ***had not begun*** under the first rule set. *See id.* at 831:24-832:3 (demonstrating that Cisco’s accused products do not cease processing packets that have already begun processing under the first (old) rule set, because “you may have to complete whatever is in flight and then you’ll stop and wait for the next step” (i.e., the second rule set)).

In this sense, Cisco’s products behave like the prior art criticized in the Background of the ’806 patent: the patent disparages network protection devices that continue processing packets in accordance with an “***outdated rule set***,” which “[i]n certain circumstances (e.g., in the event of a network attack) ... may ***exacerbate rather than mitigate the impetus for the rule set switch*** (e.g., the effect of the network attack).” JTX-2 at 1:25-31. Dr. Mitzenmacher similarly admitted that the ’806 patent was “trying to improve” on problems in prior art devices in which products continued processing packets using an outdated rule set while preparing a new rule set. Trial Tr. (Vol. 6A) (Mitzenmacher) at 815:5-816:1. This confirms that Cisco’s accused products—which continue processing packets under the old rule set during a rule swap and never “cease processing” a packet whose processing has already begun under the old rule set—do not

meet the “cease processing” limitation of the asserted claims of the ’806 patent. Cisco is entitled to judgment of non-infringement of the ’806 patent.

2. No Infringement Under the Doctrine of Equivalents

For the ’806 patent, Centripetal only referenced the doctrine of equivalents for the “preprocess” limitation of the asserted claims. *See generally* Trial Tr. (Vol. 5B) (Mitzenmacher) at 712:25-714:18. Thus, Centripetal’s doctrine of equivalents argument cannot cure the deficiencies of proof for the “cease processing” limitation and related limitations relied upon in this motion.

F. Centripetal Has Failed to Prove that the Accused Product Combinations Practice Key Limitations of U.S. Patent No. 9,686,193

Centripetal contends that the accused routers and switches⁵ infringe claims 18 and 19 of U.S. Patent No. 9,686,193 (the “’193 patent”). Trial Tr. (Vol. 4) (Mitzenmacher) at 433:20-435:20. Centripetal has failed to provide sufficient evidence to show infringement of these claims, either literally or under the doctrine of equivalents, because the accused routers and switches do not include the specific packet-filtering rule required by the first “responsive to” limitation of the asserted claims. Thus, Cisco is entitled to judgment of non-infringement with respect to the ’193 patent.

1. No Literal Infringement

Asserted claims 18 and 19 require a very specific type of rule: “one or more packet-filtering rules configured to prevent a particular type of data transfer.” This requirement appears

⁵ Although Centripetal accuses Cisco’s switches and routers alone of infringing the ’193 patent, Dr. Mitzenmacher identified the quarantine option discussed below as being associated with Cisco’s separate Stealthwatch and Identity Services Engine (ISE) offerings. Trial Tr. (Vol. 4) (Mitzenmacher) at 471:1-3.

in the first “responsive to” element. Specifically, the claims require a system or a non-transitory computer-readable medium that, inter alia, does the following things:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by *one or more packet-filtering rules configured to prevent a particular type of data transfer* from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

JTX-4 at claims 18-19.

In light of the specific items that Centripetal has accused as the “one or more packet-filtering rules configured to prevent a particular type of data transfer,” Cisco is entitled to judgment of non-infringement. There are two crucial points about Centripetal’s accusations that, taken together, are fatal to its infringement claim.

First, Centripetal accuses only the “quarantine” in Cisco’s accused products (which is issued by a human using Cisco’s Identity Services Engine (ISE)) as being the “one or more packet-filtering rules configured to prevent a particular type of data transfer.” Trial Tr. (Vol. 4) (Mitzenmacher) at 518:22-520:13, 524:14-525:3; Trial Tr. (Vol. 6A) (Mitzenmacher) at 777:23-778:15. Dr. Mitzenmacher did not identify any other aspect of the accused routers or switches that could satisfy the “one or more packet-filtering rules” requirement, and indeed conceded on cross that “I don’t recall specifically discussing others.” *Id.* at 791:17-792:1. Accordingly, the Court commented that “he has agreed that the quarantine is the only example he used of what happens when you drop a packet. So, that, he’s admitted, so let’s move on from there.” *Id.* at 792:21-24. Likewise, the quarantine is the only feature Centripetal identified in its proposed findings of fact as the “one or more packet-filtering rules configured to prevent a particular type of data transfer.” *See* Centripetal’s Findings of Fact, ¶¶ 115-124 (Dkt. 419). To establish infringement, therefore, Centripetal must show that a “quarantine” (the accused “one or more packet-filtering rules”) is “configured to prevent a particular type of data transfer,” as required by the claim.

Second, the only “particular type of data transfer” that Centripetal accused is a HyperText Transfer Protocol GET (“HTTP GET”) or a HyperText Transfer Protocol POST (“HTTP POST”) used for exfiltration. Trial Tr. (Vol. 4) (Mitzenmacher) at 520:15-17, 520:22-521:4. Dr. Mitzenmacher did not identify any other specific types of data transfer as the alleged “particular type of data transfer,” and indeed his slide summarizing his testimony confirmed that “[t]he particular type of data transfer that is prevented from quarantined computers are HTTP POST and HTTP GET commands, which are used in exfiltration attacks.” Trial Tr. (Vol 6A) (Mitzenmacher) at 786:5-787:20; *see also id.* at 779:22-780:13.

In view of these two points, Cisco is entitled to judgment of non-infringement because Dr. Mitzenmacher conceded that a quarantine (the accused packet-filtering rule) *cannot* filter packets based on the presence or absence of an HTTP POST or HTTP GET (the accused “particular type of data transfer”). As Dr. Mitzenmacher admitted, the quarantine does not examine a packet’s payload at all; it only looks at the packet’s header.⁶ Trial Tr. (Vol 6A) (Mitzenmacher) at 785:17-20 (quarantine looks at a packet’s header); Trial Tr. (Vol. 6B) (Mitzenmacher) at 870:18-21 (confirming that quarantine looks at information in the header and not the payload). But the two data transfers that Dr. Mitzenmacher accused as the “particular type of data transfer”—HTTP POST and HTTP GET—are located in a packet’s payload, not in the header. Trial Tr. (Vol 6A) (Mitzenmacher) at 780:17-23, 782:19-22; 783:14-17. By definition, the quarantine cannot be “configured to prevent” an HTTP POST or HTTP GET (“particular type of data transfer”) if it does not even search the payload for such transmissions. See Trial Tr. (Vol 6A) (Mitzenmacher) at 793:1-7 (“Q. And the quarantine rules cannot determine from a packet whether the packet has this thing we called the HTTP POST or the HTTP GET, correct? A. *I would say it might not be looking specifically for the POST or the GET*, but it’s looking at both the network address of where it’s coming from, and it may also look at the port, which would specify whether it’s HTTP or not.”).

Indeed, a quarantine is generic; it cannot identify *any particular* types of data transfer. It is instead a tool that a human being can use to block all traffic to certain destinations, regardless of the “particular type of data transfer” (and regardless of any other details about the packet).

⁶ Packets have a header and a payload. Trial Tr. (Vol 6A) (Mitzenmacher) at 780:14-16. A packet is analogous to a letter, with a “header” portion including information about the sender and the recipient (like an envelope with a return and destination address) and a “payload” that contains the substance of the communication (the letter inside an envelope).

Trial Tr. (Vol 6A) (Mitzenmacher) at 793:22-794:4; Trial Tr. (Vol 4) (Mitzenmacher) at 495:4-14 (showing a network administrator's role in quarantine). Centripetal has failed to prove that the accused switches and routers literally infringe claim 18 and 19 of the '193 patent.

2. No Infringement Under the Doctrine of Equivalents

Centripetal has also failed to demonstrate that the accused combination satisfies the “responsive to” element discussed above under the doctrine of equivalents. Dr. Mitzenmacher offered only conclusory testimony on this point. Trial Tr. (Vol. 4) (Mitzenmacher) at 550:9-551:20. He did not even attempt to explain how the quarantine option in Cisco's products, despite not being configured to target HTTP POST or HTTP GET transmissions (or indeed any particular transmissions) and despite being entirely subject to human decision-making, is nonetheless equivalent to a “packet-filtering rule” that prevents a “particular type of data transfer.” In particular, Dr. Mitzenmacher did not explain how the human-operated quarantine option operates in substantially the same way as the “packet-filtering *rule*” of the asserted claims. *See Akzo Nobel Coatings, Inc. v. Dow Chem. Co.*, 811 F.3d 1334, 1343 (Fed. Cir. 2016) (finding expert testimony “that Dow's process operates ‘in substantially the same way (by collecting the disperse material in a contained volume)’” insufficient to withstand summary judgment of no equivalents because “he fails to ... articulate how the differences between the two processes are insubstantial”). Dr. Mitzenmacher's entirely conclusory testimony, devoid of any key linking argument, cannot carry Centripetal's burden under the doctrine of equivalents. *See id.* (rejecting expert equivalents testimony that was “broad and scant” and characterized by “ambiguity and generality”). Thus, Cisco is entitled to judgment of no infringement by equivalents for the '193 patent.

IV. CENTRIPETAL HAS NOT PROVED THAT CISCO INDUCED INFRINGEMENT UNDER 35 U.S.C. § 271(b)

To prove induced infringement under 35 U.S.C. § 271(b), Centripetal must show (among other things) that Cisco *knew* that a third party's actions would constitute direct infringement of Centripetal's patents. *Commil USA, LLC v. Cisco Sys., Inc.*, 135 S. Ct. 1920, 1926 (2015) (“[L]iability for induced infringement can only attach if the defendant knew of the patent and knew as well that ‘the induced acts constitute patent infringement.’ (quoting *Global-Tech Appliances, Inc. v. SEB, S.A.*, 563 U.S. 754, 766 (2011))). The Supreme Court has explained that there is no liability for induced infringement if “the defendant reads the patent’s claims differently from the plaintiff, and that reading is reasonable”; it is not enough to assert that the defendant knows merely that the third party’s acts “might infringe.” *Id.* at 1928. Centripetal itself acknowledged that it is required to prove that Cisco “knew or willfully blinded itself to the fact that its actions were aiding and abetting direct infringement.” Centripetal’s Conclusions of Law ¶ 30 (Dkt. 419).⁷

Despite Centripetal’s recognition of its burden, not one Centripetal witness testified that Cisco knew that any third party’s actions would directly infringe. Centripetal appears to have had no plan to introduce such testimony: the “Summary Findings of Fact” that Centripetal submitted for direct examination of its witnesses do not mention this issue at all. *See* Exs. C-L (Summary Findings of Fact for Centripetal Witnesses).

Centripetal’s failure of proof is unsurprising; Cisco has reasonable (indeed correct) noninfringement positions as to all five patents, including but not limited to claim construction

⁷ Centripetal has not asserted contributory infringement under 35 U.S.C. § 271(c). *See* Centripetal’s Conclusions of Law ¶ 30 (Dkt. 419) (asserting only induced infringement under § 271(b)).

positions, which make its belief that third parties using Cisco's products do **not** infringe Centripetal's patents eminently reasonable. *See Commil*, 135 S. Ct. at 1928 (inducement liability cannot attach if "the defendant reads the patent's claims differently from the plaintiff, and that reading is reasonable"); *Ecolab, Inc. v. FMC Corp.*, 569 F.3d 1335, 1351, *amended on reh'g in part*, 366 F. App'x 154 (Fed. Cir. 2009) (defendant's reasonable belief of non-infringement was sufficient evidence that defendant lacked the intent required for induced infringement); *DSU Med. Corp. v. JMS Co.*, 471 F.3d 1293, 1307 (Fed. Cir. 2006) (where defendant "did not believe its [product] infringed," evidence showed a "lack of the necessary specific intent" required for inducement). Cisco's reasonable noninfringement defenses include but are not limited to the points developed in Part III above. Whether or not the Court accepts Cisco's noninfringement arguments, they are at the very least **reasonable** and accordingly defeat any assertion that Cisco **knew** or was **willfully blind** to direct infringement by third parties.

Centripetal accordingly provided the Court with no basis to find that Cisco induced infringement of any Centripetal patent under 35 U.S.C. § 271(b). The Court should accordingly enter judgment of no induced infringement.

V. CONCLUSION

For the foregoing reasons, the Court should enter judgment on partial findings that Centripetal has failed to prove direct infringement of all asserted patents and has likewise failed to prove induced infringement of all asserted patents.

Dated: May 21, 2020

CISCO SYSTEMS, INC.

By /s/ _____
Of Counsel

Dabney J. Carr, IV, VSB No. 28679
TROUTMAN SANDERS LLP
P. O. Box 1122
Richmond, Virginia 23218-1122
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
dabney.carr@troutmansanders.com

Neil H. MacBride, VSB No. 79883
DAVIS POLK & WARDWELL LLP
901 15th Street, NW
Washington, DC 20005
Telephone: (202) 962-7000
Facsimile: (202) 962-7111
neil.macbride@davispolk.com

Louis N. Jameson (admitted pro hac vice)
Matthew C. Gaudet (admitted pro hac vice)
John R. Gibson, VSB No. 72968
Jennifer H. Forte (admitted pro hac vice)
DUANE MORRIS, LLP
1075 Peachtree Street, N.E., Suite 2000
Atlanta, Georgia 30309-3929
Telephone: (404) 253-6900
Facsimile: (404) 253-6901
wjameson@duanemorris.com
jrgibson@duanemorris.com
jhforte@duanemorris.com

Joseph A. Powers (admitted pro hac vice)
DUANE MORRIS, LLP
30 South 17th Street
Philadelphia, PA 19103-4196
Telephone: (215) 979-1000
Facsimile: (215) 689-3797
japowers@duanemorris.com

Nicole E. Grigg (formerly Johnson) (admitted pro hac vice)
DUANE MORRIS, LLP
2475 Hanover Street
Palo Alto, CA 94304-1194
Telephone: (650) 847-4150
Facsimile: (650) 618-2713
NEGrigg@duanemorris.com

Counsel for Defendant Cisco Systems, Inc.